Concld
A1

memory and storing said variable x_1 in said first register, the reading of a variable x_3 from said second memory and storing said variable x_3 in said third register, and the reading of a variable x_5 from said third memory and storing said variable x_5 in said fifth register.

16. (original) The arithmetic method according to claim 15, wherein said first memory is a two-port memory having one data writing port and one data reading port, while said second and third memories are single-port memories having one port for the writing and reading of data.

****

Kindly amend the Figure 7 as indicated on the attached sheet.

Remarks

The above amendment is submitted in response to the office action dated February 13, 2003.

Applicants enclose a revised Figure 7 where the label "Prior Art" has been added. Applicants submit that the amendment does not add any new matter to the disclosure. Applicants submit that the drawings are now in compliance with MPEP 808.02(g).

The invention centers on circuits and methods which are especially useful for boosting the speed of Montgomery multiplication (which uses a large-digit number such as a 1024-bit number) without the need for extraordinary circuits such as a three port memory. The invention involves the discovery that memory access is a bottleneck which can be overcome by simultaneous reading from at least two memori s in a way which is coordinated with the overall pipeline

Received from < 845 892 6363 > at 6/12/03 3:54:18 PM [Eastern Daylight Time]

process employed by the arithmetic unit in performing the Montgomery multiplication.

USP4,955,024 discloses a patent for a display system that processes a high-speed transmission and mask operations for image data stream. The display system in USP4,955,024 has parallel buses to store and read-back a large amount of image data to a memory, and to speed up a shift/mask operation. USP4,955,024 uses adders and multiplier adders to calculate the address of image data, which is stored in a memory, from X- and Y-coordinate information. The adders and the multiplier-adders are just used to calculate the memory address of image data, not to calculate the image data itself.

Claims 1-16 are rejected under 35 U.S.C. 102(b) as being anticipated by Pfeiffer et al, (U.S.4,955,024).

In USP4,955,024, the arithmetic units 146 and 148 calculate the x-coordinate and y-coordinate of image data. The four-port register file 144 is used to store the processed x- and y-coordinates. These x- and y-coordinates are processed independently, and the bit width of the x- and y- coordinate is no more than 32 bits. With regard to the image processing computer in USP4,955,024, image data are stored in the image memory 82, and the arithmetic units 146 and 148 are not used to process these image data. USP4,955,024 does not disclose or the connection between the arithmetic unit and the registers and memories as presently claimed, i.e., where the register values are accessed as inputs to the arithmetic unit and multiple variables are read from the plural memories to the same set of registers.

Re claims 2 and 10: In USP4,955,024, the arithmetic unit 146 that is an adder receives data from the output port A of the four-port memory 144, and calculates

Received from < 845 892 6363 > at 6/12/03 3:54:18 PM [Eastern Daylight Time]

a new y-coordinate of image data. The multiplier adder 150 calculates a linear address for the image memory 82 by using x-coordinate from the output port B of 144, and y-coordinate data from the output port A of 144. The renewed y-coordinate and the linear address are written back to the memory 144 through the input port C. The output data from the arithmetic unit 148 is fed back to the input port D of 144. The four-port memory 144 has only two read ports A and B, and thus the multiplication-addition X1+X2*X3+X4 claimed in our patent cannot be executed by the data path disclosed in USP4,955,024.

Re claims 3 and 11: In USP4,955,024, the memory 226 is a part of the image memory 82, which holds a special area not shown on a displayed. On the other hand, the first memory and the second memory in our claims are independent. They and are used to supply consecutive data to a multiplier adder in parallel to prevent disruption of operation flow. The four-port memory 144 of USP4,955,024 stores x- and y-coordinates for the image memory 82 (and its partial area 226), and these coordinates and picture image are different type of data. Therefore, the arithmetic units 146, 148, and 150 for the coordinate data do not process the data in the image memory. USP4,955,024 does not disclose or suggest that the data stored in the registers have dependencies and are processed by using the only one multiplier adder.

Re claims 4 and 12: USP4,955,024 discloses in col. 11 that a two-port memory can be used in order to increase the transmission bandwidth of the image memory 82. One port is used for random read/write operations of image processing, and the other port is for sequential read operations to refresh a display. These read and/or write operations are executed independently. On the contrary, two two-port memories in our claims increase the performance of the arithmetic unit (multiplier-adder). By using two two-port memories and some temporary registers, many data blocks are supplied efficiently to the multiplier adder, and the result is write back to the memories and/or the registers in every clock cycle without disrupting the multiplication.

Re claims 5 and 13: In USP4,955,024, the two-port memory 82 stores image data, and the single-port memory 464 stores microinstructions that are decoded and executed in a sequential order. Therefore, the use of these two memories is completely different. Claims 5 and 13 of the present invention encompass the concept that hardware resource can be reduced with minor declining of operating speed by replacing one of the two two-port memories in claims 4 and 12 by a single-port memory.

Re claims 6 and 14: Claims 6 and 14 describe the way to double the processing performance in comparison with claims 2 and 10 by efficiently feeding six r-bit numbers X1, X2, X3, X4, X5 and X6 to a multiplier adder that calculates 2r-bit or (2r+1)-bit number. The adders 146, and 148, and the multiplier adder 150 in USP4,955,024 just calculate coordinates on a display. Table V(a) defines the data selection field in microinstructions for the coordinates calculation. Table VI just defines the bit assignment (bit width and its meaning) of microinstructions, and thus no arithmetic operations are executed on these fields defined by the Tables. Six registers in Fig.31 are used by the image processor 72 to just control mask operations as described in col.60. Therefore these registers are not used for arithmetic operations.

Re claims 7 and 15: The two memories 82 and 226 in USP4,955,024 are not discreet memories as described as "a portion of the image memory 82 is 226" at col. 20 line 43-46 in USP4,955,024. The register 627 is the 8-bit register, where the upper 5 bits specify the shift-width of image processing, and the lower 3 bits are used for the expander control. On the other hand, the term Q in our claims specifies the integer value that is a result of iterative arithmetic operations.

Therefore, its upper bits Qh and lower bits Ql have completely different meaning compared to the lower and upper bits of the register 627. In addition, the register 629 in the Fig. 31 stores a bit mask pattern, and thus there is no arithmetic relationship between the data in the registers 227 and 229.

Re claims 8 and 16: USP4,955,024 teaches a system, wherein the first memory 82 is a two-port memory having one data writing port and one data reading port (col. 11, lines 41-53), while the second memory is a single-port memory 464 having one port for the writing and data reading (col. 38, lines 61-68 and col. 39, lines 1-68). USP4,955,024 does not disclose or suggest the relationship between memory registers and arithmetic unit required by the present claims. USP4,955,024 does not disclose or suggest that hardware resource can be reduced by replacing two-port memories by single-port memories with minor declining of the performance speed.

For the above reasons, applicants submit that the claims are allowable over the prior art of record and that the application is now in condition for allowance. Such allowance is earnestly and respectfully solicited.

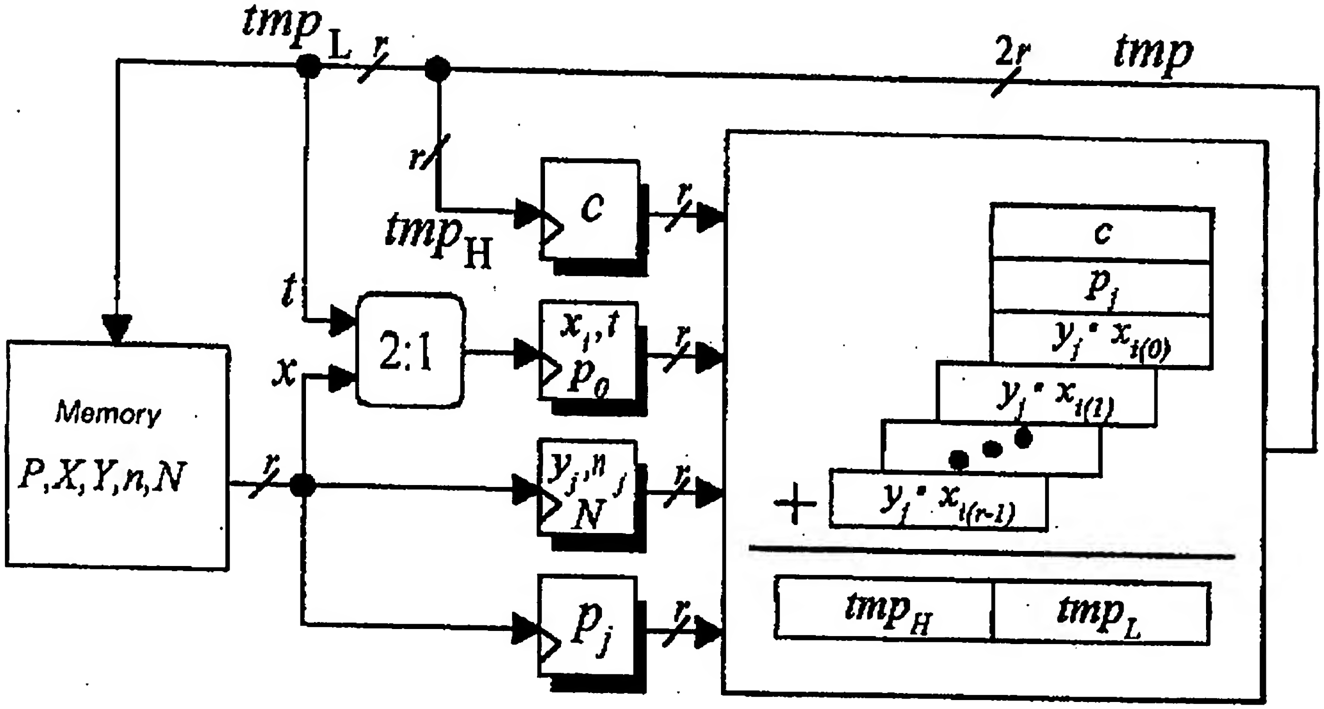
Respectfully submitted,
Kohji Takano et al.

By Steven Capella
Steven Capella, Attorney
Reg. No. 33,086
Telephone: 845-894-3669

Received from < 845 892 6363 > at 6/12/03 3:54:18 PM [Eastern Daylight Time]

10/023,147

Amended



$$tmp \leftarrow p_j + x_i \cdot y_j + c$$
$$tmp \leftarrow p_j + t \cdot n_j + c$$
$$tmp \leftarrow p_0 \cdot N$$

PRIOR ART

Fig. 7